

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF NEBRASKA

UNITED STATES OF AMERICA,

Plaintiff,

vs.

ALL CRYPTOCURRENCY, VIRTUAL  
CURRENCY, FUNDS, MONIES, AND  
OTHER THINGS OF VALUE STORED IN  
OR ACCESSIBLE AT BINANCE  
ASSOCIATED WITH USER ID #  
39344718.

Defendant.

Civil No. 8:23CV75

**COMPLAINT FOR FORFEITURE *IN REM***

The United States of America, for its cause of action against the defendant property, pursuant to Rule G(2) of the Supplemental Rules for Admiralty and Maritime Claims and Asset Forfeiture Actions, states and alleges as follows:

**Nature of the Action**

1. This is an action to forfeit property to the United States for violations of 18 U.S.C. § 981(a)(1)(A) and (C).

**The Defendant *in rem***

2. Defendant property is all present and future interest in the following property: cryptocurrency, virtual currency, funds, monies, and other things of value (hereinafter “the Cryptocurrency”) previously stored under the user identification number: 39344718<sup>1</sup>, by Binance Holdings Ltd d.b.a. “Binance” (which owns and operates the Binance cryptocurrency exchange).

---

<sup>1</sup> As of on or about February 10, 2022, User ID: 39344718 had three (3) cryptocurrency assets seized by FBI to include Asset ID numbers: 22-FBI-002388, 22-FBI-002895, and 22-FBI-

3. The Cryptocurrency was seized by the Federal Bureau of Investigation (hereinafter “FBI”) in the District of Nebraska pursuant to a federal seizure warrant for forfeiture that was executed on Binance in or around February 10, 2022.
4. The FBI currently has custody of the defendant property in an FBI controlled account.

**Jurisdiction and Venue**

5. This Court has subject matter jurisdiction for an action commenced by the United States pursuant to 28 U.S.C. § 1345, and for an action for forfeiture pursuant to 28 U.S.C. § 1355(a).
6. This Court has *in rem* jurisdiction over the defendant property pursuant to 28 U.S.C. § 1355(b).
7. Venue is proper in this district pursuant to 28 U.S.C. §§ 1355 and 1395 because acts or omissions giving rise to the forfeiture occurred in this district.

**Basis for the Forfeiture**

8. This action seeks the forfeiture of all right, title, and interest in the above-captioned property because the property constitutes or is derived from proceeds of wire fraud and wire fraud conspiracy in violation of 18 U.S.C. §§ 1343 and 1349, and property involved in monetary transactions and money laundering conspiracy in violation of 18 U.S.C. §§ 1956 and 1957.

## Facts

### **Background on Cryptocurrency**

9. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys (described below) used to transfer cryptocurrency from one person or place to another can be printed or written on a piece of paper or other tangible object. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries.
10. Generally, cryptocurrency is not issued by any government, bank, or company. Instead, cryptocurrency is generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a “blockchain,” which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction. Cryptocurrency is not illegal in the United States.
11. Bitcoin (“BTC”) is a type of cryptocurrency. Payments or transfers of value made with bitcoin are recorded in the Bitcoin blockchain and thus are not maintained by any single administrator or entity. As mentioned above, individuals can acquire bitcoin through exchanges (i.e., online companies that allow individuals to buy or sell cryptocurrencies in exchange for fiat currencies<sup>2</sup> or other cryptocurrencies), bitcoin ATMs, or directly from other people. Individuals can also acquire cryptocurrencies by “mining.” An individual can “mine” bitcoins by using his or her computing power to solve a complicated algorithm and

---

<sup>2</sup> Fiat currency is currency issued and regulated by a government such as the U.S. Dollar, Euro, or Japanese Yen.

verify and record payments on the blockchain. Individuals are rewarded for this task by receiving newly created units of a cryptocurrency. Individuals can send and receive cryptocurrencies online using many types of electronic devices, including laptop computers and smart phones. Even though the public addresses of those engaging in cryptocurrency transactions are recorded on a blockchain, the identities of the individuals or entities behind the public addresses are not recorded on these public ledgers. If, however, an individual or entity is linked to a public address, it may be possible to determine what transactions were conducted by that individual or entity. Bitcoin transactions are therefore sometimes described as “pseudonymous,” meaning that they are partially anonymous. And although bitcoin transactions are not completely anonymous, bitcoin does allow users to transfer funds more anonymously than traditional financial transactions.

12. Cryptocurrency is stored in a virtual account called a wallet. Wallets are software programs that interface with blockchains and then generate, store, or generate and store public and private keys used to send and receive cryptocurrency. A public key, or public address, is akin to a bank account number, and a private key, or private address, is akin to a PIN number or password that allows a user to access and transfer value associated with the public address or key.
13. To conduct transactions on a blockchain, an individual must use the public address as well as the private key. A public address is represented as a case-sensitive string of letters and numbers, 26–35 characters long. Each public address is controlled and/or accessed through the use of a unique corresponding private key—the cryptographic equivalent of a password or PIN—needed to access the address. Only the holder of a public address’s private key can

authorize any transfers of cryptocurrency from that cryptocurrency public address to another cryptocurrency address.

14. Although cryptocurrencies such as bitcoin have legitimate uses, cryptocurrency is frequently used by individuals and organizations for criminal purposes, such as to pay for illegal goods and services – via, for example, hidden services websites operating on the Tor network.
15. Cryptocurrencies can also be used to engage in money laundering. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement’s efforts to track purchases within the dark web marketplaces.
16. Exchangers and users of cryptocurrencies store and transact their cryptocurrency in accounts commonly referred to as “wallets,” which are essentially digital accounts. A cryptocurrency user can store and access wallet software in a variety of forms, including via:
  - a PC or laptop (“desktop wallet”),
  - a mobile application on a smartphone or tablet (“mobile wallet”),
  - an Internet-based cloud storage provider (“online wallet”),
  - an online account associated with a cryptocurrency exchange (“online account”),
  - a tangible, external device, such as a USB thumb drive (“hardware wallet”), or
  - printed public and private keys (“paper wallet”).
17. Because these desktop, mobile, and online wallets are electronic in nature, they are located on mobile devices (e.g., smart phones or tablets) or at websites that users can access via a computer, smart phone, or any device that can search the Internet. Moreover, hardware wallets are located on some type of external or removable media device, such as a USB thumb drive or other commercially available device designed to store cryptocurrency (e.g., Trezor, Keepkey, or Nano Ledger). In addition, paper wallets contain an address and a QR

code with the public and private key embedded in the code. Paper wallet keys are not stored digitally.

18. Wallets can also be backed up via, for example, paper printouts, USB drives, or CDs. Wallets can be accessed through a password or a “recovery seed” or “mnemonic phrase,” that is, random words strung together in a phrase.
19. Additional security safeguards for cryptocurrency wallets can include two-factor authorization, such as a password and a phrase. FBI Special Agent Rachel Sullivan (“SA Sullivan”) knows that based on her training and experience that individuals possessing cryptocurrencies often have safeguards in place to prevent their assets from hacking, unauthorized transfer, and/or law enforcement seizure.
20. “Ethereum” is a cryptocurrency, or virtual currency, that utilizes a blockchain-based software program. Ethereum is the world's second-largest cryptocurrency by market capitalization, behind Bitcoin.
21. “TetherUS” (USDT), as referred to as “Tether”, is a cryptocurrency purportedly backed by United States dollars. Tether was originally designed to always be worth \$1, and the company responsible for issuing Tether purportedly maintained \$1 in reserves for each Tether issued.
22. Cryptocurrency transactions can have multiple inputs and multiple outputs. While the ownership of any particular address or wallet can be anonymous, all transactions of cryptocurrencies are recorded on a "blockchain," which is a series of "blocks" of transactions that establishes a verifiable, transparent record of the movement of virtual currency. Blockchains in this context are viewable by the public-they show all transactions,

but do not reflect who owns a particular address. As cryptocurrency transactions are processed, they are assigned a unique identifier on the blockchain called a transaction hash.

23. Cryptocurrency exchanges exist and operate similarly to fiat currency exchanges. Customers use these exchanges to trade one form of digital currency for another, or to exchange digital currency into fiat money. In SA Sullivan's training, knowledge, and experience, fraudsters will use cryptocurrency exchanges to launder or obfuscate their illicit gains.
24. Based on the training and experience of SA Sullivan, she knows that financial account information, including cryptocurrency wallets, is not typically shared across multiple, unrelated individuals. Based on SA Sullivan's training and experience, she further knows that this shared use of information is very often the same person or a close and trusted group working in concert.
25. Further, based on SA Sullivan's training and experience, she knows that individuals engaged in criminal activity involving cryptocurrency frequently engage in "chain hopping," meaning that they convert funds from one cryptocurrency to another, in order to obscure the source of funds and make it more difficult to track illicit funds as they move from one blockchain to another.

### **Background on Binance**

26. Binance Holding Limited ("Binance"), which is registered and domiciled in the Cayman Islands, owns and operates Binance.com, a cryptocurrency exchange that provides a platform for trading various cryptocurrencies and exchanging cryptocurrencies for fiat currencies. Binance is one of the largest cryptocurrency exchanges in the world based on its

trading volume. Among other services, Binance maintains the private keys relating to the customer's cryptocurrency and therefore has complete control over client funds.

27. Customers use exchanges like Binance to trade one form of digital currency for another, such as exchanging Ethereum for other digital currencies or to exchange digital currencies into fiat money.

#### **Summary of the Scheme Involving the Victim**

28. On September 2, 2021, local law enforcement notified the FBI about a virtual currency scam that had occurred in Omaha, Nebraska.
29. The victim, M.M. (hereinafter "Victim") met an individual named Stefan Lang on an online dating platform who convinced her to invest her savings into cryptocurrency.
30. Starting in June 2021 through August 2021, the Victim deposited approximately \$732,937.10 United States dollars (USD) into Bitcoin and then sent approximately 20.227 Bitcoin to the Bitcoin Miner, named Michael Girard.
31. The Victim attempted to "cash-out" her Bitcoin wallets but was told by Girard that she must provide an 18% clearance fee in order to receive the funds.
32. The Victim sent the clearance fee in three installments.
33. The Victim did not receive her funds.
34. Rather, after completing the alleged required 18% clearance fee, she was told the exchange system was automated and required the clearance fee be paid in one transaction.
35. After this point, the Victim reported the suspicious activity to local law enforcement.

36. Through the investigation, FBI identified nine (9) Target Accounts at Binance that facilitated the wire fraud and money laundering scheme against the victim. Those Target Accounts<sup>3</sup> included:

**TARGET ACCOUNT 1**

- User ID: 36597019
- Associated Email Address: gideonaigbokhan@gmail.com
- Wallet: 1B4DrEkTAohtpuhC5HfYjCPe8BCS5711Tp (**5711Tp**)

**TARGET ACCOUNT 2**

- User ID: 43195807
- Associated Email Address: busolaponle@gmail.com
- Wallet: 1FMq6aAzV9TLzN6pQR8nY4zecxPV8ysap2 (**8ysap2**)

**TARGET ACCOUNT 3**

- User ID: 92386528
- Associated Email Address: lincho5000@gmail.com
- Wallet: 18SnDM11nJ8MhqdShneJ6XAUBQJ31oAWgA (**1oAWgA**)

**TARGET ACCOUNT 4**

- User ID: 39344718
- Associated Email Address: chironuah@gmail.com
- Wallet: 16BCSenn8vGDDuZdDPRUEyGXxTYQhz1Em1 (**Qhz1Em1**)

**TARGET ACCOUNT 5**

- User ID: 74696451
- Associated Email Address: ng09043430386\_mobileuser@binance.com
- Wallet: 1Fq89kYH6V17ASMdDvuhi7KL5WBgE1J5SU (**E1J5SU**)

**TARGET ACCOUNT 6**

- User ID: 37608436
- Associated Email Address: donomoba@gmail.com
- Wallet: 1MDDKSMVFnoznWjyzEp1pKuD6RAtTwQoAd (**TwQoAd**)

**TARGET ACCOUNT 7**

- User ID: 57037490
- Associated Email Address: utpo12345@gmail.com
- Wallet: 1H1b1yiUoKc1oFKughvQRZ1GgDX6PnRCGK (**PnRcGK**)

---

<sup>3</sup> The Target Account at issue in this civil complaint is Target Account 4 as that is the only user ID that has submitted a claim for seized cryptocurrency in this case.

**TARGET ACCOUNT 8**

- User ID: 75836931
- Associated Email Address: danyaljavanmard1199@gmail.com
- Wallet: 1PNmeE5KPZWKpy4m4bVcBm1sZba2WR3asF (**WR3asF**)

**TARGET ACCOUNT 9**

- User ID: 35013532
- Associated Email Address: nefsccharlie7@gmail.com
- Wallet: 16VfQWFgpQdK6wxT8QobWu1Wc3AV6jZc6g (**6jZc6g**)

37. Through further investigation, FBI linked these Target Accounts to the following User IDs<sup>4</sup>, individuals, cryptocurrency type, and cryptocurrency amounts just prior to seizure in February 2022 (See Figure 1):

User ID	User Name	Cryptocurrency	Crypto Amount
92386528	MICHAEL EMMANUEL OKERE	TetherUS (USDT)	47199.7703
92386528	MICHAEL EMMANUEL OKERE	Cosmos (ATOM)	0.00383
User ID	User Name	Cryptocurrency	Crypto Amount
39344718	TOBENNA NEWTON OKOLO	TetherUS (USDT)	20935.78263
39344718	TOBENNA NEWTON OKOLO	Bitcoin (BTC)	0.17696577
39344718	TOBENNA NEWTON OKOLO	Binance Coin (BNB)	15.61181818
User ID	User Name	Cryptocurrency	Crypto Amount
36597019	GIDEON OSEGHALE AIGBOKHAN	Ethereum (ETH)	0.76215244
36597019	GIDEON OSEGHALE AIGBOKHAN	TetherUS (USDT)	626.7826
36597019	GIDEON OSEGHALE AIGBOKHAN	Binance Coin (BNB)	2.69573253
36597019	GIDEON OSEGHALE AIGBOKHAN	Ripple (XRP)	330.43877
36597019	GIDEON OSEGHALE AIGBOKHAN	Theta Token (THETA)	45.036
36597019	GIDEON OSEGHALE AIGBOKHAN	Origin Token (OGN)	219.59
36597019	GIDEON OSEGHALE AIGBOKHAN	Polygon (MATIC)	122.9
36597019	GIDEON OSEGHALE AIGBOKHAN	TRON (TRX)	2044.437672
36597019	GIDEON OSEGHALE AIGBOKHAN	DREP (DREP)	143.407
36597019	GIDEON OSEGHALE AIGBOKHAN	Dogecoin (DOGE)	718.696

<sup>4</sup> The specific User ID at issue in this civil forfeiture case is 39344718.

36597019	GIDEON OSEGHALE AIGBOKHAN	VeChain (VET)	1113.3
36597019	GIDEON OSEGHALE AIGBOKHAN	Swipe (SXP)	50.06
<b>UserID</b>	<b>User Name</b>	Cryptocurrency	Crypto Amount
35013532	CHARLES EJIMOFOR MBANEFO	eCash (XEC)	55649273.02
35013532	CHARLES EJIMOFOR MBANEFO	TetherUS (USDT)	2584.5213
35013532	CHARLES EJIMOFOR MBANEFO	Bitcoin (BTC)	0.01218667
<b>UserID</b>	<b>User Name</b>	Cryptocurrency	Crypto Amount
43195807	BUSOLA AKASILI	Aragon (ANT)	196.4411
43195807	BUSOLA AKASILI	Avalanche (AVAX)	6.433263
43195807	BUSOLA AKASILI	Automata (ATA)	515.036
43195807	BUSOLA AKASILI	Cardano (ADA)	360.24099
43195807	BUSOLA AKASILI	AION (AION)	2504.72335
43195807	BUSOLA AKASILI	IOST (IOST)	10201.161
43195807	BUSOLA AKASILI	Bakery Token (BAKE)	198.3037
43195807	BUSOLA AKASILI	Aave (AAVE)	1.1833189
43195807	BUSOLA AKASILI	Ripple (XRP)	244.689
43195807	BUSOLA AKASILI	Smooth Love Potion (SLP)	4129.626
43195807	BUSOLA AKASILI	Tezos (XTZ)	41.38569
43195807	BUSOLA AKASILI	FTX Token (FTT)	4.092172
43195807	BUSOLA AKASILI	Reserve Rights (RSR)	4020.3222
43195807	BUSOLA AKASILI	Litecoin (LTC)	0.92674562
43195807	BUSOLA AKASILI	Mdex (MDX)	218.57132
43195807	BUSOLA AKASILI	Internet Computer (ICP)	2.80478
43195807	BUSOLA AKASILI	Solana (SOL)	0.725989
43195807	BUSOLA AKASILI	Theta Token (THETA)	22.284938
43195807	BUSOLA AKASILI	Dogecoin (DOGE)	666.342
<b>UserID</b>	<b>User Name</b>	Cryptocurrency	Crypto Amount
37608436	JESSE OSAMUDIAMEN OSAGIE	Bitcoin (BTC)	0.01305
37608436	JESSE OSAMUDIAMEN OSAGIE	TetherUS (USDT)	243.0181
<b>UserID</b>	<b>User Name</b>	Cryptocurrency	Crypto Amount
75836931	DOMINIQUE BAUDIS	TetherUS (USDT)	747.0588235

<b>UserID</b>	<b>User Name</b>	Cryptocurrency	Crypto Amount
57037490	TAIYE UWUIGBE	Bitcoin (BTC)	0.00940228
57037490	TAIYE UWUIGBE	TetherUS (USDT)	498.10206
<b>UserID</b>	<b>User Name</b>	Cryptocurrency	Crypto Amount
74696451	EMMANUEL OLUWATOMINI DANIEL	TetherUS (USDT)	5.403627
74696451	EMMANUEL OLUWATOMINI DANIEL	Binance Coin (BNB)	0.00590107

(Figure 1)

38. In particular, on June 2, 2021, the Victim converted \$14,990.00 United States dollars through Coinbase to 0.39227349 Bitcoin (BTC) and sent 0.38804781 BTC to receiving address 1FMqYAv76yTEAoyU4LC2s86eYSRE9hLMaV (hLMaV).

39. From June 2, 2021 to August 23, 2021, a series of exchanges occurred to address ending in hLMaV totaling five transactions in the amount of 11.3085 BTC.

40. On July 1, 2021, the Victim converted \$199,990.00 through Coinbase to 5.87613932 BTC and sent 5.87611392 BTC to receiving address 1PRXttWfoxVnGtPYQwUSh5mQN1Zxm1FFub (m1FFub). From July 1, 2021 to July 26, 2021, a series of exchanges occurred to an address ending in (m1FFub) totaling three transactions in the amount of 8.9189 BTC. (See Figures 2 and 3).

Date	Coinbase Deposit	VC Type Purchase	VC Amount	Receiving Address	VC Type	VC Amt	Fee Amt	VC Total
6/2/2021	\$14,990.00	BTC	0.39227349	1FMqYAv76yTEAoyU4LC2s86eYSRE9hLMaV	BTC	0.388048	0.00001393	0.388062
6/4/2021	\$19,990.00	BTC	0.52958548	1FMqYAv76yTEAoyU4LC2s86eYSRE9hLMaV	BTC	0.533783	0.00001371	0.533797
6/18/2021	\$99,990.00	BTC	2.76382624	1FMqYAv76yTEAoyU4LC2s86eYSRE9hLMaV	BTC	2.763816	0.00001023	2.763826
6/24/2021	\$199,990.00	BTC	5.62811288	1FMqYAv76yTEAoyU4LC2s86eYSRE9hLMaV	BTC	5.628095	0.00001848	5.628113
7/1/2021	\$199,990.00	BTC	5.87613932	1PRXttWfoxVnGtPYQwUSh5mQN1Zxm1FFub	BTC	5.876114	0.00002586	5.87614
7/19/2021	\$84,990.00	BTC	2.72210464	1PRXttWfoxVnGtPYQwUSh5mQN1Zxm1FFub	BTC	2.722104	0.00000103	2.722105
7/26/2021	\$12,990.00	BTC	0.32073382	1PRXttWfoxVnGtPYQwUSh5mQN1Zxm1FFub	BTC	0.320732	0.00000232	0.320734
8/23/2021	\$100,007.10	BTC	1.99476363	1FMqYAv76yTEAoyU4LC2s86eYSRE9hLMaV	BTC	1.994763	0.00000089	1.994764
<b>Total</b>	<b>\$732,937.10</b>		<b>20.2275395</b>		<b>Total</b>		<b>20.22745</b>	<b>0.00008645</b>
								<b>20.22754</b>

(Figure 2)

Receiving Address	VC Type	VC Amount	Trans Count
1FMqYAv76yTEAoyU4LC2s86eYSRE9hLMaV	BTC	11.3085	5
1PRXttWfoxVnGtPYQwUSh5mQN1Zxm1FFub	BTC	8.9189	3
<b>Total</b>		<b>20.2274</b>	<b>8</b>

(Figure 3)

41. After the funds were transferred to the wallets ending in (hLMaV) and (m1FFub), the subject or subjects executed a series of transfers that resulted in multiple types of virtual currency, such as USDT (Tether) sent by the Victim being routed to Binance wallet addresses.
42. Per a search of the public block chain, (hLMaV) and (m1FFub) received 20.2274532 BTC.
43. As of October 21, 2021, these addresses had a combined balance of 0.003 BTC.
44. Using publicly available block chain information, the FBI traced a minimum of 16.5579 BTC from the Victim's Coinbase account to Target Accounts below held at Binance.
45. The accounts below contained the deposit addresses that were held in multiple virtual currencies with total BTC equivalent to the value of 2.20936709 BTC. For reference, as of February 7, 2022, one Bitcoin was trading for \$43,360.80 USD which totaled \$95,799.92 to be seized. Cryptocurrency is a fluid currency and changes minute-by-minute similar to the stock market. (See Figure 4).

UserID	BTC Deposit Address	Binance AcctBalance (in BTC Equiv)
92386528	18SnDM11nJ8MhqdShneJ6XAUBQJ31oAWgA	0.73774
39344718	16BCSenn8vGDDuZdDPRUEyGXxTYQhz1Em1	0.6559
74696451	1Fq89kYH6V17ASMDvuh17KL5WBgE1J5SU	0.00008709
37608436	1MDDKSMVFnoznWjyzEp1pKuD6RAtTwQoAd	0.01542
57037490	1H1b1yiUoKc1oFKughvQRZ1GgDX6PnRCGK	0.00778
75836931	1PNmeE5KPZWKpy4m4bVcbm1sZba2WR3asF	0.2113
36597019	1B4DrEkTAohtpuhC5HfYjCPe8BCS5711Tp	0.1779
43195807	1FMq6aAzV9TLzN6pQR8nY4zecxPV8ysap2	0.17344
35013532	16VfQWFgpQdK6wxT8QobWu1Wc3AV6jZc6g	0.2298
<b>Total</b>		<b>2.20936709</b>

(Figure 4)

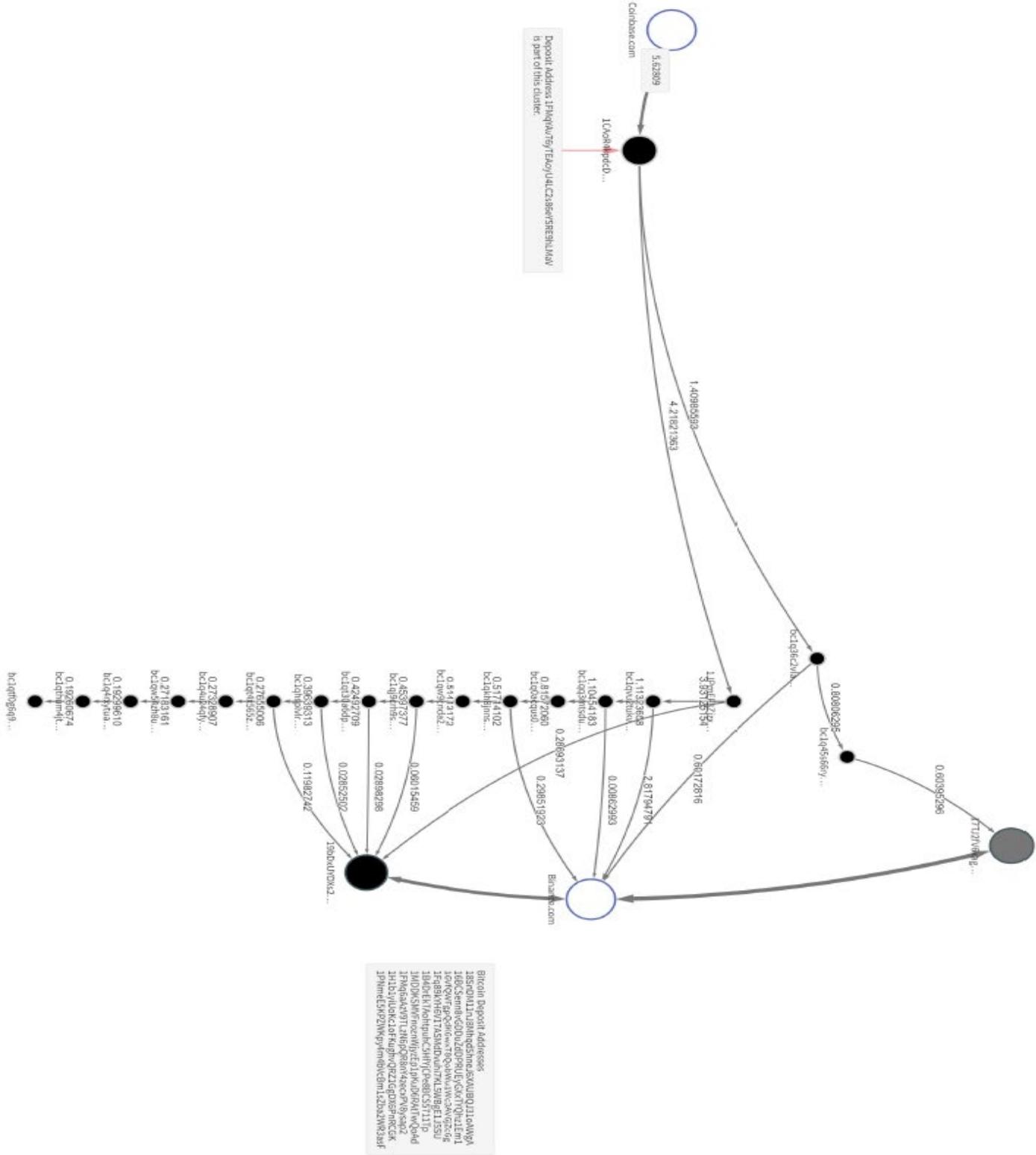
46. Beginning on September 9, 2021, SA Sullivan sent emails to Binance requesting Binance to voluntarily provide account and ownership associated with the Binance wallet addresses for the target accounts identified as target accounts 1, 2, 3, 4, 5, 6, 7, 8, and 9, and restrain or freeze the funds in Binance wallet addresses for target accounts 1, 2, 3, 4, 5, 6, 7, 8, and 9.

47. On October 6, 2021, October 11, 2021, and October 20, 2021, Binance employee Victoria, email address victoria@binance.com, provided spreadsheets to the FBI that indicated Binance wallets associated with the following user IDs and emails (See Figure 5):

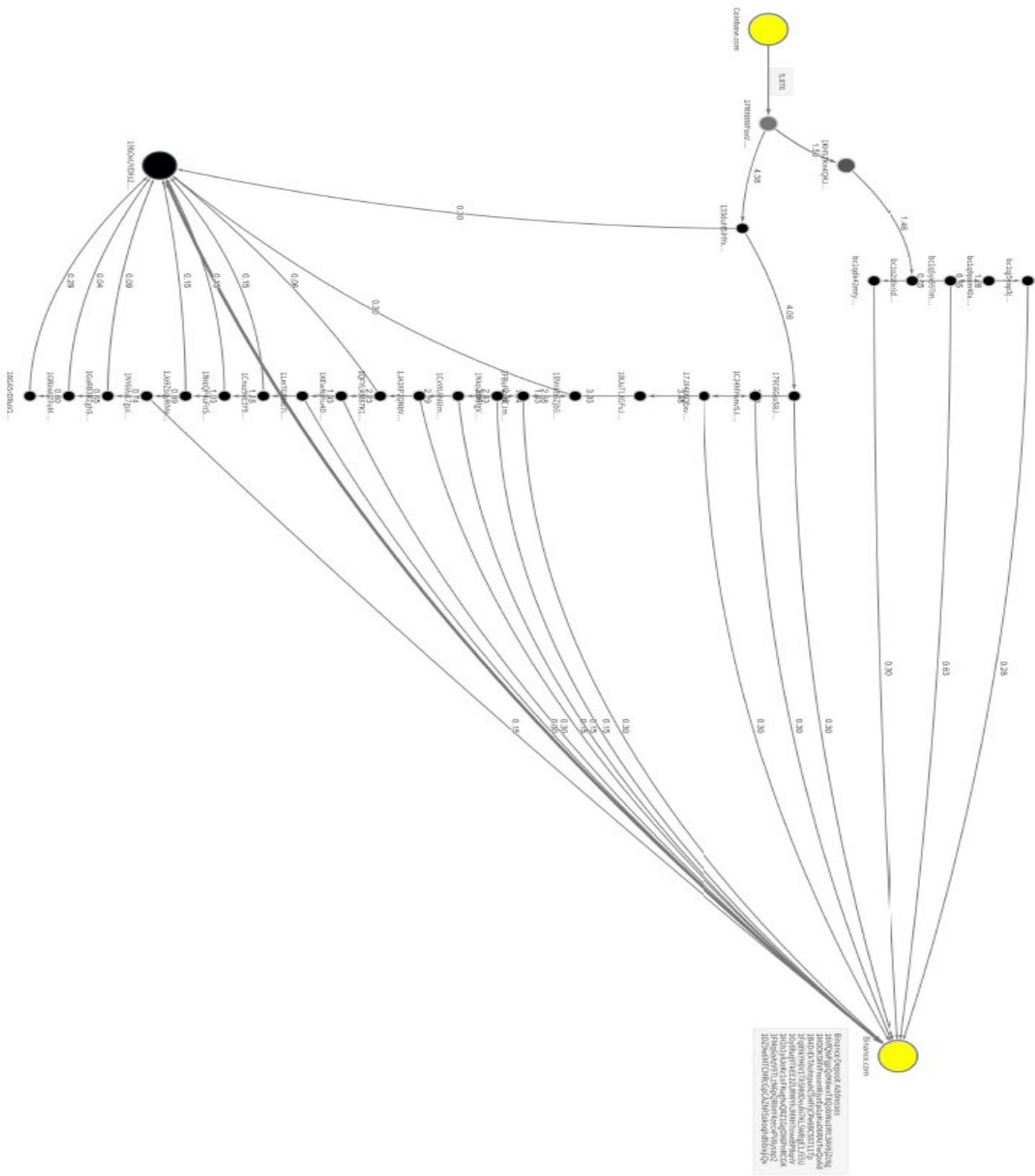
UserID	User Email
92386528	lincho5000@gmail.com
39344718	chironuah@gmail.com
74696451	ng09043430386_mobileuser@binance.com
37608436	donomoba@gmail.com
57037490	utpo12345@gmail.com
75836931	danyaljavanmard1199@gmail.com
36597019	gideonaiqbokhan@gmail.com
43195807	busolaponle@gmail.com
35013532	nefscharlie7@gmail.com

(Figure 5)

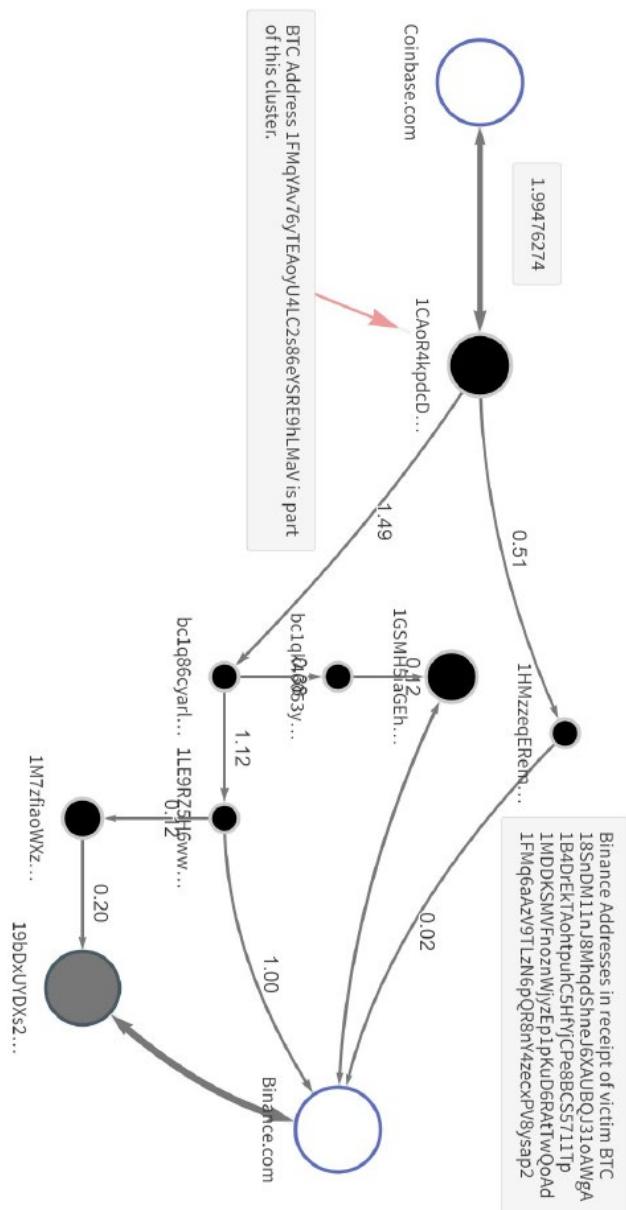
48. Victoria also confirmed that all funds or assets in the above Binance wallet Target Accounts had been frozen.
49. See Figures 6-13 below for examples of traced Bitcoin from transactions between the Victim and the Target Accounts held at Binance.



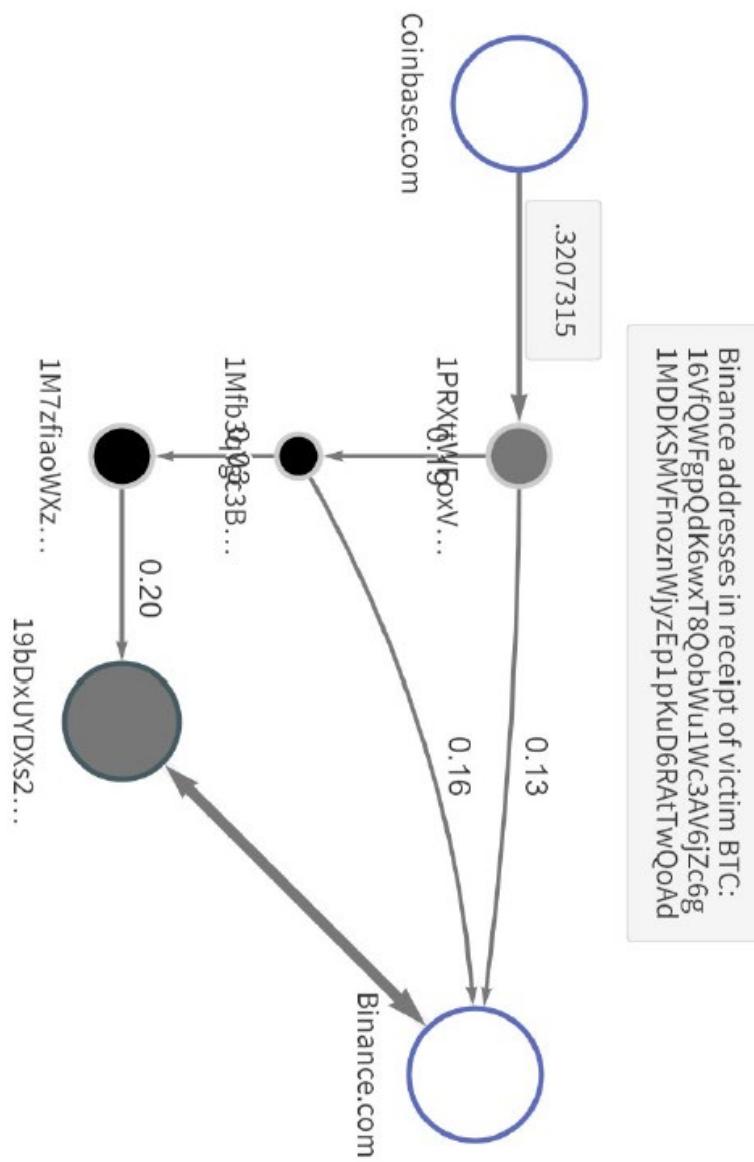
(Figure 6)



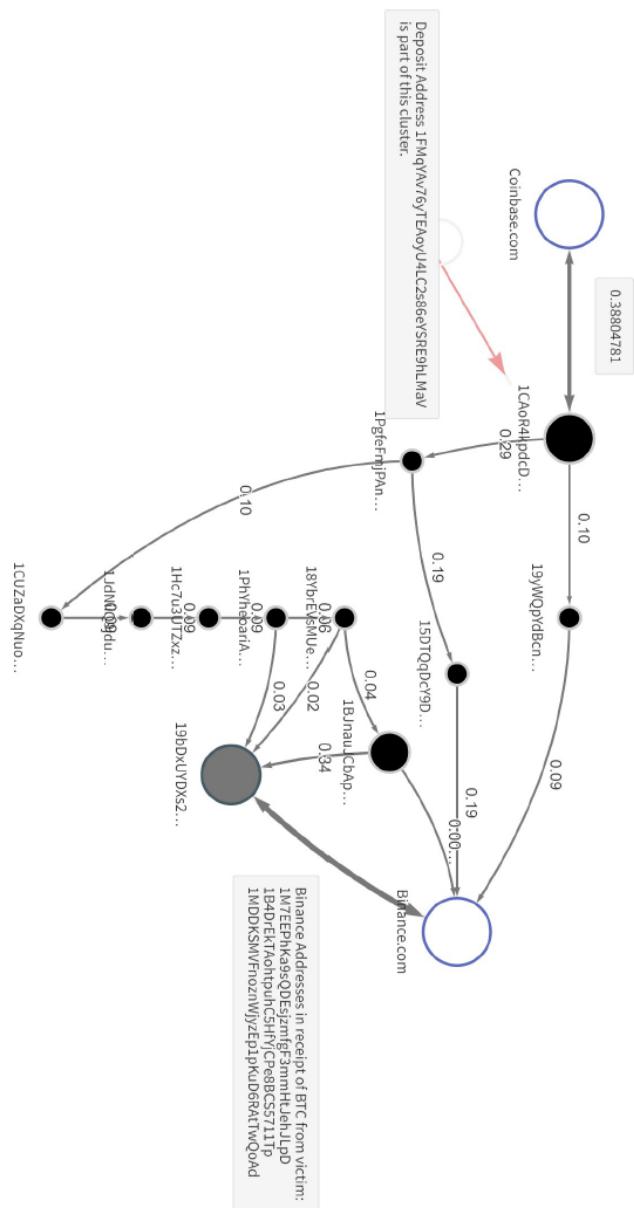
(Figure 7)



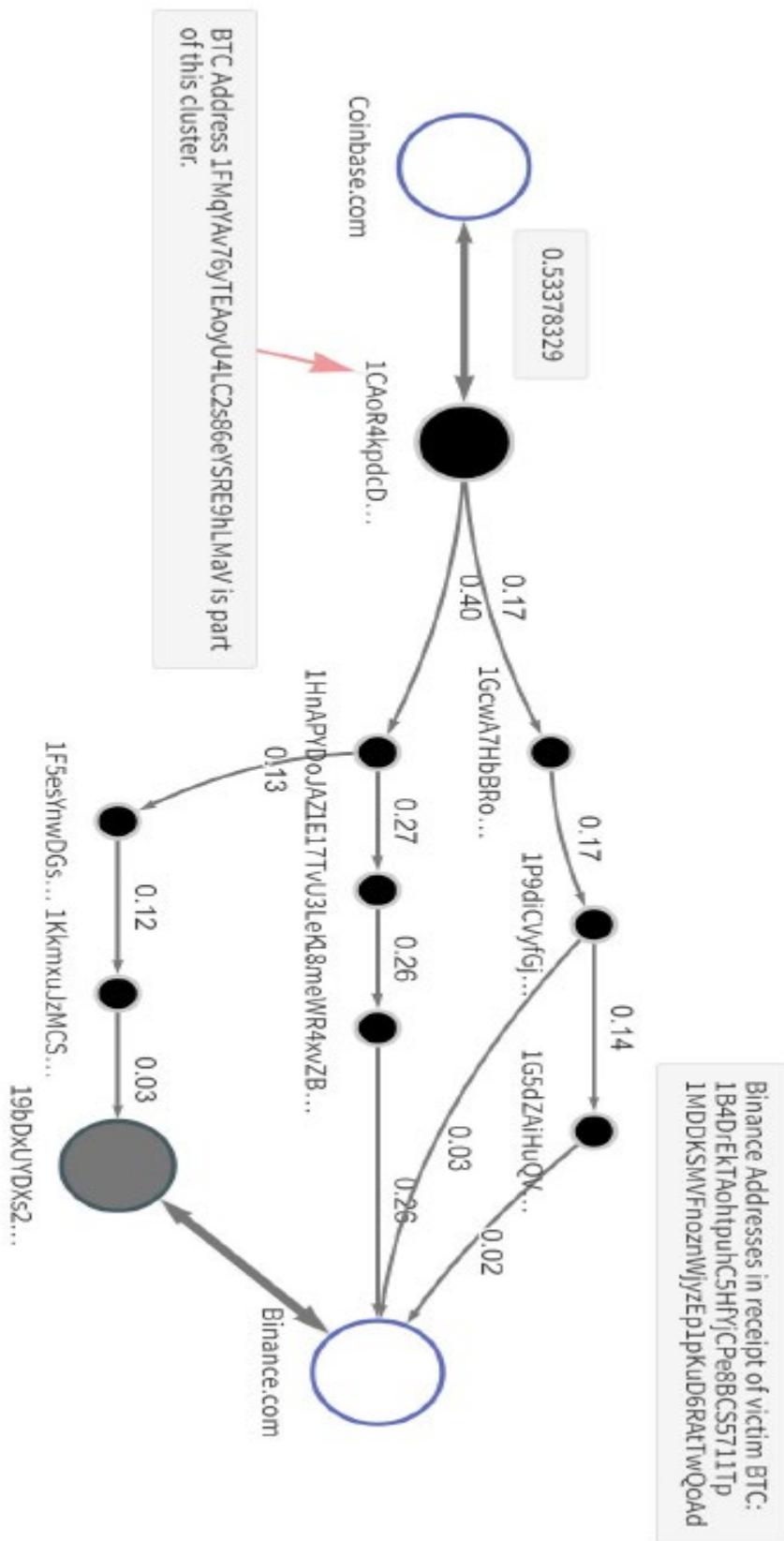
(Figure 8)



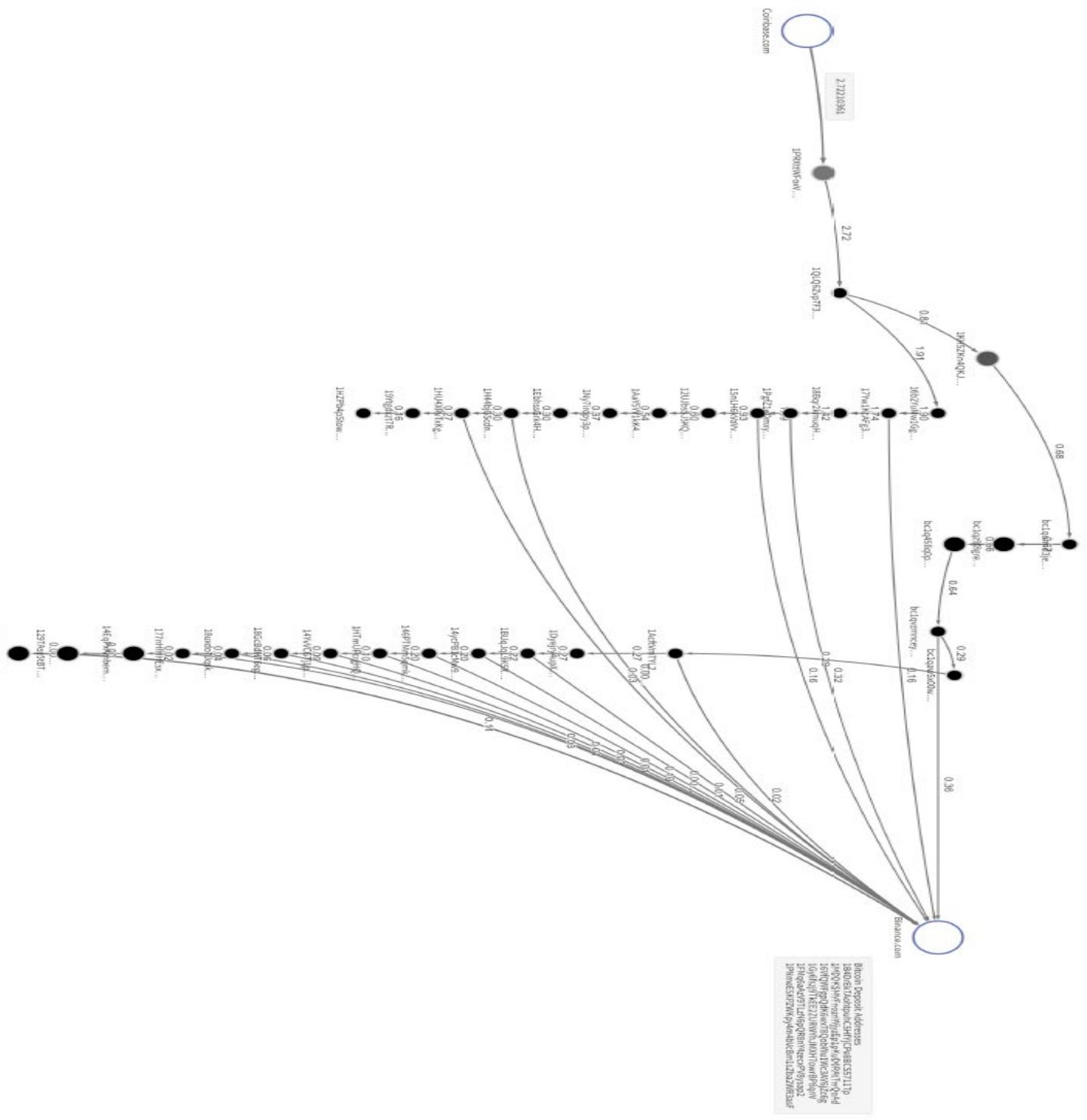
(Figure 9)



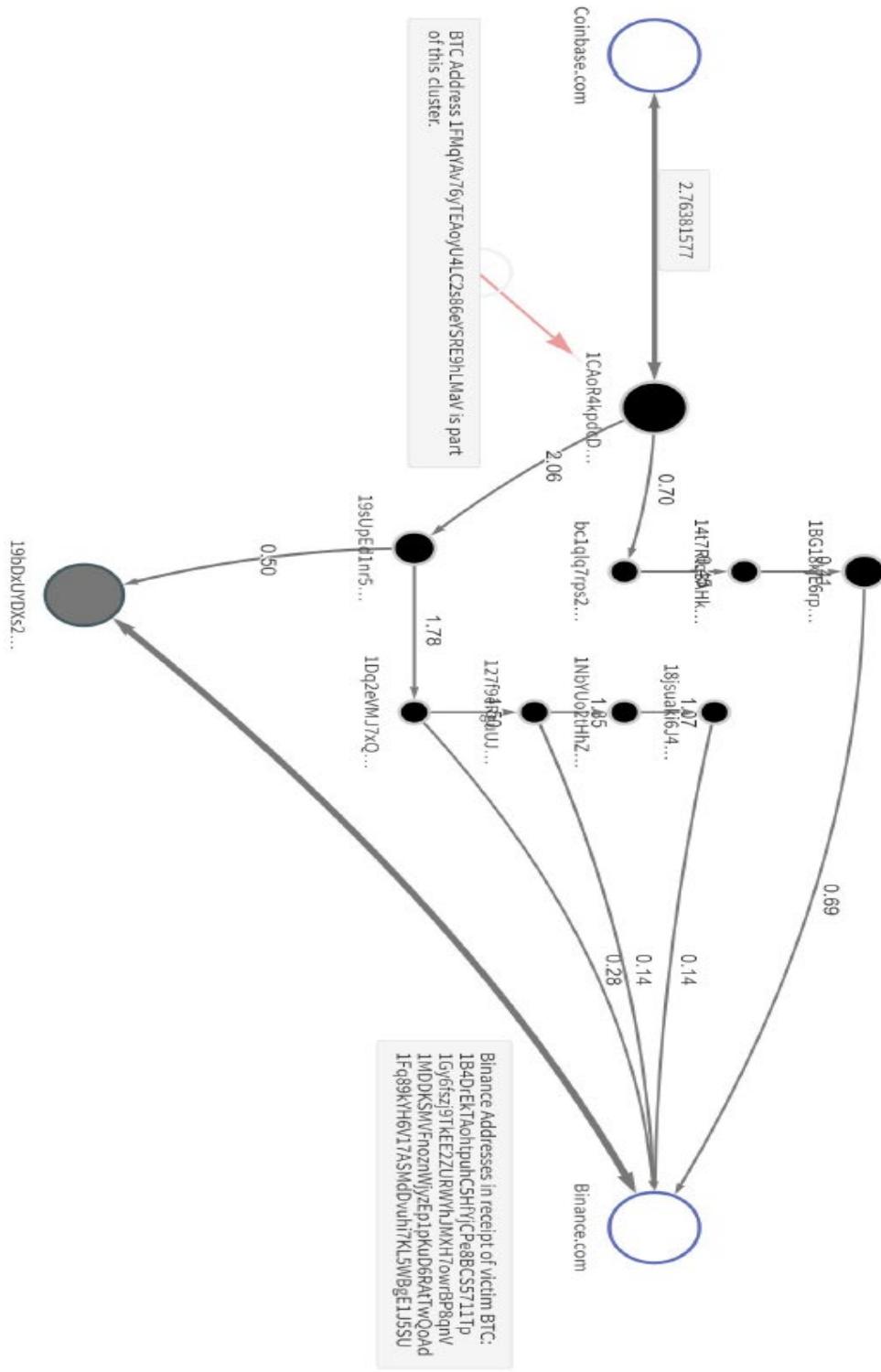
(Figure 10)



(Figure 11)



(Figure 12)



(Figure 13)

50. On or about November 11, 2021, FBI secured a properly authorized federal seizure warrant for the Target Accounts. However, Binance did not comply with this seizure warrant.
51. On or about February 10, 2022, FBI executed a second properly authorized federal seizure warrant on the Target Accounts and directed Binance to place the contents of the Target Accounts in an FBI controlled account.
52. Evidence obtained in the FBI's investigation demonstrates that there is probable cause to believe that the Victim, an Omaha, Nebraska resident, had been victimized in a wire fraud scheme that violated 18 U.S.C. §§ 1343 and 1349, and money laundering scheme in violation of 18 U.S.C. §§ 1956 and 1957.
53. Based on the above facts and circumstances, there is probable cause to believe the funds in Binance Holdings Limited in the seized user account 39344718 is subject to seizure and forfeiture pursuant to Title 18, U.S.C, Sections 981(a)(1)(A) and (C) on grounds the funds were derived from proceeds traceable to a violation of wire fraud and wire fraud conspiracy, 18 U.S.C. §§ 1343 and 1349, and property involved in monetary transactions and money laundering conspiracy in violation of 18 U.S.C. §§ 1956 and 1957.

#### **Claim for Relief**

WHEREFORE the United States of America prays the defendant property be proceeded against for forfeiture in accordance with the laws, regulations and rules of this Court; that due notice be given to all interested parties to appear and show cause why forfeiture should not be decreed; that the defendant property be condemned, as forfeited, to the United States of America and disposed of according to law and regulations; that the costs of this action be assessed against

the defendant property; and for such other and further relief as this Court may deem just and equitable.

UNITED STATES OF AMERICA,  
Plaintiff

STEVEN A. RUSSELL  
United States Attorney

By: s/ Mikala Purdy-Steenholdt  
MIKALA PURDY-STEENHOLDT  
(NY#5112289)  
Assistant U.S. Attorney  
1620 Dodge Street, Suite 1400  
Omaha, NE 68102-1506  
Tel: (402) 661-3700  
Fax: (402) 345-5724  
Email: [Mikala.Purdy-Steenholdt@usdoj.gov](mailto:Mikala.Purdy-Steenholdt@usdoj.gov)

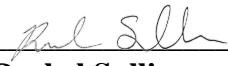
**VERIFICATION**

I, Special Agent Rachel Sullivan, hereby verify and declare under penalty of perjury that I am a Special Agent with the Federal Bureau of Investigation (“FBI”), that I have read the foregoing Verified Complaint *in Rem* and know the contents thereof, and that the factual matters contained in paragraphs 9 through 53 of the Verified Complaint are true to my own knowledge, except that those matters herein stated to be alleged on information and belief and as to those matters I believe them to be true.

The sources of my knowledge and information and the grounds of my belief are the official files and records of the United States, information supplied to me by other law enforcement officers, as well as my investigation of this case, together with others, as a Special Agent of the FBI.

I hereby verify and declare under penalty of perjury that the foregoing is true and correct.

Dated: February 28, 2023.

  
**Rachel Sullivan**  
Special Agent  
FBI